PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-114787
(43)Date of publication of application : 02.05.1997

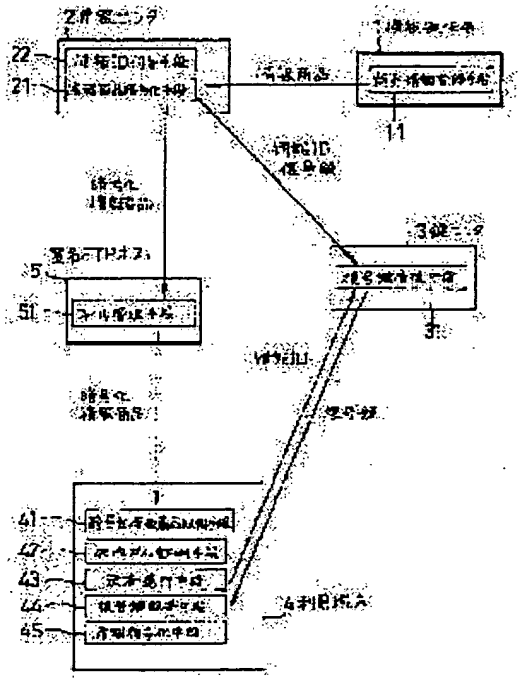
(51)Int.Cl. G06F 15/00
G06F 9/06
G06F 17/60
G09C 1/00
H04L 9/08

(21)Application number : 07-274324
(22)Date of filing : 23.10.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : AKASHI OSAMU
MORIYASU KENJI
TERAUCHI ATSUSHI

(54) METHOD AND SYSTEM FOR INFORMATION DISTRIBUTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information distribution method and system capable of performing the authentication and settlement of accounts as necessary and referring to information by decoding the information being a ciphered article by using the decoding key obtained from a key center and utilizing the information.
SOLUTION: An information center 2 ciphers the provided information and imparts information identification ID to the ciphered information article. A key center 3 receives the information identification ID and a decoding key from the information center 2, controls them, receives the settlement of accounts from an arbitrary information use terminal and returns the key for decoding the information article in exchange for the reception to a using terminal. A using terminal 4 obtains identifier and the ciphered information article and confirms that the information is not fraudulently altered by authenticator. When the decision of obtaining the information article is performed corresponding to the identifier part or the reception is performed, the charge for the information article is paid before the decoding of information. As for the key for a decoding in exchange for the payment, the decoded key is received from the key center 3 by keeping the key secret from a third party by using the secret communication system combined a public key with a secret key.



LEGAL STATUS

[Date of request for examination] 17.11.1998
[Date of sending the examiner's decision of rejection] 18.09.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－114787

(43)公開日　平成９年(1997)５月２日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｚ
	9/06	５５０			9/06	５５０Ａ
	17/60		7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｄ
Ｇ０９Ｃ	1/00	６３０		Ｇ０６Ｆ	15/21	Ｚ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｄ

審査請求　未請求　請求項の数５　ＯＬ　（全６頁）

(21)出願番号　特願平7－274324

(22)出願日　平成７年(1995)10月23日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　明石　修
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　森保　健治
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　寺内　敦
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

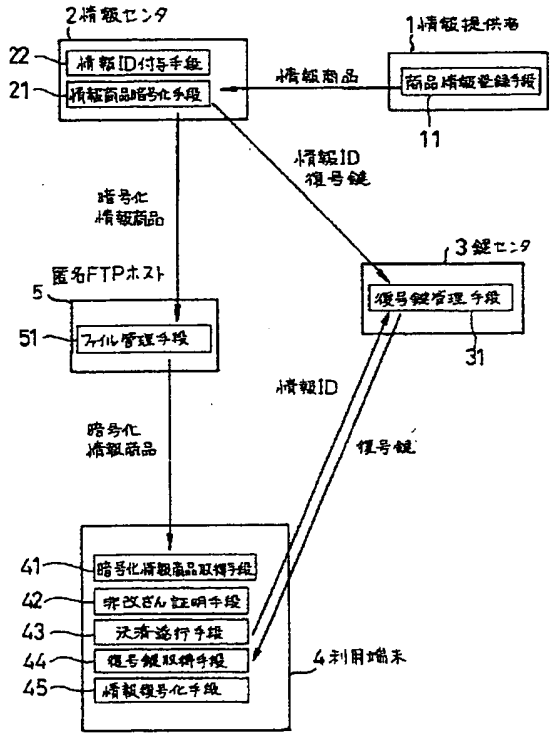
(74)代理人　弁理士　若林　忠

(54)【発明の名称】　情報流通方法及びシステム

(57)【要約】

【課題】　情報を保護した上で、ネットワーク上の任意の場所に置くことを可能とし、必要に応じて認証および決済を行い、情報を参照することの出来るような情報流通方法及びシステムを提供すること

【解決手段】　商品である情報は暗号化した保護状態で情報センタに登録しておき、情報を参照したい利用端末からは、ネットワークを通じて前記情報センタにアクセスし、該当する暗号化された情報を得た後で、該情報の復号化に先立ってネットワークを通じて該情報に対する電子的な料金支払を鍵センタに対して行う。次に利用端末は、該支払と引き換えに復号化の鍵を、鍵センタとの間で公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して鍵センタからネットワークを通じて得る。更に利用端末は、得た復号化の鍵を用いて上記情報を復号化し、利用することを特徴とする。



1

【 特許請求の範囲】

【 請求項1 】　商品である情報は、暗号化することにより保護し、認証子関数を用いて改ざんを検知可能とした状態で情報センタに登録し、ネットワーク上に自由に配布し、

該商品である情報の利用端末は、ネットワークを通じて前記情報センタあるいは商品である情報が配布された計算機にアクセスし、該当する暗号化された情報を得、

該利用端末は、該情報の復号化に先立ってネットワークを通じて該情報に対する電子的な料金支払を鍵センタに対して行い、

該利用端末は、該支払と引き換えに復号化の鍵を、該鍵センタと該利用端末の間で公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して鍵センタからネットワークを通じて得、

該利用端末は、得た復号化の鍵を用いて上記情報を復号化し、利用することを特徴とする情報流通方法。

【 請求項2 】　前記商品である情報の暗号化及び秘密通信方式に適用する暗号方式として、公開鍵暗号方式と秘密鍵暗号方式を組合せて用いることを特徴とする請求項1 記載の情報流通方法。

【 請求項3 】　商品である情報を暗号化することにより保護し、認証子関数を用いて改ざんを検知可能とした状態で、該情報商品の識別子とともに記憶保持する情報センタと、

任意の情報利用端末からの決済を受付け、受付と引き替えに上記情報商品を復号化するための鍵を該利用端末に返送する鍵センタと、

前記識別子及び暗号化された情報商品を得る情報商品取得手段と、上記識別子部分に呼応して上記情報商品を得る判定を行った、または受付けた場合には、該情報の復号化に先立って該情報商品に対する料金支払を行う決済遂行手段と、該支払と引き替えに復号化のための鍵を、公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して前記鍵センタから受け取る復号鍵取得手段と、該復号化のための鍵により上記情報商品を復号化する情報復号化手段と、外部と通信し情報を送受するためのネットワークインターフェース手段とを具備する複数の情報利用端末と、

前記の情報センタ、任意の情報利用端末及び鍵センタの間で情報を送受する媒介となる情報ネットワークとから構成されることを特徴とする情報流通システム。

【 請求項4 】　上記の情報センタは、商品である情報の一部を暗号化することにより保護した状態で記憶保持し、

上記の情報利用端末の情報商品取得手段は、上記一部を暗号化した情報商品を得、暗号化していない部分に呼応して、上記情報商品を得る判定を行った、または受付けた場合に、上記決済遂行手段を起動することを特徴とする請求項3 記載の情報流通システム。

2

【 請求項5 】　前記商品である情報の暗号化及び秘密通信方式に適用する暗号方式として、公開鍵暗号方式と秘密鍵暗号方式を組合せて用いることを特徴とする請求項3 または4 記載の情報流通システム。

【 発明の詳細な説明】

【０００１】

【 発明の属する技術分野】本発明は、任意の情報を任意のユーザが自由に登録でき、暗号により情報を保護した状態でネットワーク上を自由に流通させ、情報の参照時に料金決済を行い復号鍵を配布することにより情報参照を可能とする情報流通方法及びそのシステムに関する。

【０００２】

【 従来の技術】従来、情報をインターネット上の特定のセンタに置いておき、情報を参照したい者は、そのセンタにネットワークを経由してアクセスし、認証および決済処理を行い、その後に情報を転送することによって情報を入手していた。

【０００３】あるいは、暗号化した情報をＣＤ－ＲＯＭに入れて配布し、情報を参照したいユーザは、その復号鍵を管理するセンタにアクセスし、認証および決済処理を行なった後、復号鍵を入手することにより、情報を得ていた。

【０００４】情報を特定のセンタに置いておく方法は、情報の配布先が認証および決済機能のあるセンタに限定され、情報を得ようとする者は必ずそのセンタにアクセスする必要があり、アクセスが集中するという問題がある。しかもそのセンタにおいてユーザアクセス管理や、認証、課金処理に加えて情報転送までも行うので、計算機やネットワークに大きな負荷が掛かることになる。また、情報自体は自分の計算機に置いておき、情報の参照毎に利用料金を払うような利用形態には適用が不可能である。

【０００５】また、暗号化した情報をＣＤ－ＲＯＭに入れて配布する方法は、情報の提供者はＣＤ－ＲＯＭを発行し流通させるコストが必要となる。ＣＤ－ＲＯＭ発行元が複数の情報をまとめることで1 情報当たりのコストを下げることも可能であるが、情報の取りまとめや管理といった新たなコストも生じる。またＣＤ－ＲＯＭは物理的な媒体なので、発行や流通過程での時間コストも大きい、という問題がある。

【０００６】

【 発明が解決しようとする課題】上述したように、情報を特定のセンタに置いておく方法は、アクセスが集中してしまい、計算機やネットワークに大きな負荷をかけるという問題がある。また、情報自体は自分の計算機に置いておき、情報の参照毎に料金を支払うような利用形態には適用が不可能である。このため情報を保護した上で、ネットワーク上の任意の場所に置くことを可能とし、必要に応じて認証および決済を行い、情報を参照することの出来るような情報流通方式が必要である。

3

【０００７】また、暗号化した情報をＣＤ－ＲＯＭに入れて配布する方法は、情報の提供者はＣＤ－ＲＯＭを発行し流通させるコストが必要であるという問題がある。またＣＤ－ＲＯＭは物理的な媒体なので、発行や流通過程での時間コストも大きいという問題もある。したがて、特定の大きな組織ではなく、一般のユーザがネットワーク上で簡単に情報を登録でき、最終的に情報の参照者から料金を徴収する方法が必要である。

【０００８】本発明は、上記の必要からなされたもので、一般のユーザがネットワーク上で簡単に登録できる情報を保護した上で、ネットワーク上の任意の場所に置くことを可能とし、必要に応じて認証および決済を行い、情報を参照することの出来るような情報流通方法及びシステムを提供することを目的としている。

【０００９】

【課題を解決するための手段】上記課題を解決するために、本発明の情報流通方法は、商品である情報は、暗号化することにより保護した状態で情報センタに登録して置き、該商品である情報の利用端末は、ネットワークを通じて前記情報センタにアクセスし、該当する暗号化された情報を得、該利用端末は、該情報の復号化に先立ってネットワークを通じて該情報に対する電子的な料金支払を鍵センタに対して行い、該利用端末は、該支払と引き換えに復号化の鍵を、該鍵センタと該利用端末の間で公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して鍵センタからネットワークを通じて得、該利用端末は、得た復号化の鍵を用いて上記情報を復号化し、利用することを特徴とする。

【００１０】また、本発明の情報流通システムは、商品である情報を暗号化することにより保護し、認証子関数を用いて改ざんを検知可能とした状態で、該情報商品の識別子とともに記憶保持する情報センタと、任意の情報利用端末からの決済を受付け、受付と引き替えに上記情報商品を復号化するための鍵を該利用端末に返送する鍵センタと、前記識別子及び暗号化された情報商品を得る情報商品取得手段と、上記識別子部分に呼応して上記情報商品を得る判定を行った、または受付けた場合には、該情報の復号化に先立って該情報商品に対する料金支払を行う決済遂行手段と、該支払と引き替えに復号化のための鍵を、公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して前記鍵センタから受け取る復号鍵取得手段と、該復号化のための鍵により上記情報商品を復号化する情報復号化手段と、外部と通信し情報を送受するためのネットワークインターフェース手段とを具備する複数の情報利用端末と、前記の情報センタ、任意の情報利用端末及び鍵センタの間で情報を送受する媒介となる情報ネットワークとから構成されることを特徴とする。

【００１１】本発明によれば、情報の整形処理は特定のセンタで行うが、そのセンタへのアクセスは情報の登録

4

時のみであり、暗号化の後は自由にネットワーク上に配布することが可能であるため、ネットワークへの負荷は分散することになる。また、参照毎に料金を支払うような利用形態でも、情報自体は自分の計算機に置いておき、認証、決済、復号鍵の配送等を行えばよい。また、ネットワーク中を自由に配布させるため、第三者による改ざんや情報が混入する可能性があるが、ディジタル署名と認証子関数により、それらは検知可能である。認証および決済処理と復号鍵の配布を行う鍵センタは登録センタと同一の計算機である必要がないので、計算負荷およびネットワーク負荷は分散することができる。

【００１２】

【発明の実施の形態】本発明について図面を用いて説明する。図1は本発明の実施形態の実施例の構成を示すブロック図、図2は実施例の構成における動作手順を示すフローチャートである。

【００１３】図1において、１は、情報を商品として情報センタ２へ商品情報登録手段１１を介して提供する情報提供者である。２は、提供された情報を暗号化し認証子関数により第三者による改ざんから保護できる形に整形する情報商品暗号化手段２１、暗号化した情報商品に識別子を付する情報ＩＤ付与手段２２等を有する情報センタである。３は、情報センタ２から情報識別子ＩＤ、復号鍵を受けて管理する復号鍵管理手段３１を有し、任意の情報利用端末からの決済を受付け、受付と引替えに情報商品を復号化するための鍵を利用端末に返送する鍵センタである。

【００１４】４は複数ある利用端末であり、各利用端末は、識別子及び暗号化された情報商品を得る情報商品取得手段４１、認証子により改ざんされてないことを確認する非改ざん証明手段４２、識別子部分に呼応して情報商品を得る判定を行った、または受付けた場合には、情報の復号化に先立って情報商品に対する料金支払を行う決済遂行手段４３、支払と引き替えに復号化のための鍵を、公開鍵と秘密鍵を組合せた秘密通信方式を用い、第三者に秘して前記鍵センタ３から受け取る復号鍵取得手段４４、復号化のための鍵により情報商品を復号化する情報復号化手段４５、および外部と通信し情報を送受するためのネットワークインターフェース手段とを具備している。

【００１５】５は、情報センタ２より配布され暗号化情報商品のファイル管理手段５１を有し、情報商品を利用端末に提供する匿名ＦＴＰホストである。前記の情報センタ２、任意の情報利用端末1あるいは4、鍵センタ３および匿名ＦＴＰホスト５の間は、情報ネットワークを媒介して結ばれている。

【００１６】次に、実施例における動作手順について、図2を参照して説明する。

【００１７】情報センタ１は、情報提供者が情報の登録を行う場所である。登録処理（ステップ１）では、情報

5

のアップロード、情報料金の払込先等の決済のための情報の入力を行う。情報センタはこれらの情報を1つのかたまりとしてまとめ、カプセルを生成する。本実施例では、カプセルは制御情報をディジタル署名して生成したヘッダ部と、暗号化した情報本体から成るデータ部とでなる。

【００１８】ヘッダ部Hは公開鍵暗号方式によるディジタル署名により生成する。この公開鍵暗号Fp( ) はディジタル署名が可能であるような全単射の関数を用いるが、その公開している公開鍵Kpと、それと対をなす秘密鍵Ksを持つ。公開鍵暗号Fp( ) は全単射の性質を持つため、公開鍵Kpで暗号化した文は秘密鍵Ksで復号でき、逆に秘密鍵Ksで暗号化した文は公開鍵Kpで復号できる。

【００１９】また、情報センタでは、配布する情報本体を暗号化する（ステップ2）。この暗号には秘密鍵暗号方式Fsec( ) と鍵Ksecを用いて、Dsec =Fsec(情報本体、鍵Ksec) を生成する。このDsecが暗号化したデータ部である。情報本体の復号は、秘密鍵暗号方式Fsec( ) に鍵Ksecを適用し、Fsec(Dsec、鍵Ksec) で行う。

【００２０】次に、データ部Dsecの全てのビットに依存した値を生成し、あるデータDに対してFa(D) = Fa(D′) となるDと等しくないD′を見つけることが困難であるような性質を持つ認証子関数Fa( ) を用い、認証子Va =Fa(Dsec) を計算する。次にこの情報本体に一意に定まる情報識別子IDiを付与し（ステップ2）情報識別子IDi、鍵Ksecを鍵センタに送る（ステップ3）。

【００２１】一方、制御情報に認証子Va、情報識別子IDiおよび鍵センタのアドレスを設定した後、秘密鍵Ksによりヘッダ部H＝公開鍵暗号 Fp(制御情報、秘密鍵Ks) を計算する。このヘッダ部Hとデータ部Dsecを結合したデータが、配布するカプセルとして、匿名FTPホストに配布される（ステップ4）。

【００２２】情報センタはカプセルを生成後、商品として匿名FTPホストに配布するが、このカプセル化された情報は上記したようにディジタル署名と認証子関数Fa( ) により改ざんを防止してあるため、匿名FTPホストのように通常インターネットで用いられているファイル集積／配布のためのシステムを用いることが可能となる。

【００２３】情報を参照したい者は、公開されている公開鍵Kpにより制御情報＝公開鍵暗号Fp（ヘッダ部H、公開鍵Kp）で制御情報を取り出すことが可能であるが、情報センタ以外は秘密鍵Ksを知らないので、ヘッダ部Hを生成することが不可能であるため、ヘッダ部Hは情報センタで生成された情報であり、なおかつ第三者により改ざんもされていないことも確認される。

6

【００２４】実際には、情報を参照したいユーザは、情報センタあるい匿名FTPホストにアクセスし、必要な情報をFTP等の通常の転送プロトコルを用いダウンロードする（ステップ5）。端末側では、公開されている公開鍵Kpにより制御情報＝公開鍵暗号 Fp(ヘッダ部H、公開鍵Kp) で制御情報を取り出し、復号に必要な鍵センタのアドレス、認証子Va、情報識別子IDiを得る。

【００２５】次に、改ざんされていないことを確認するため、先の認証子Vaと認証子関数Fa( ) によりデータ部Dsecを再計算した結果Va′からVa=Va′を確認する。改ざんされていないことが確認された場合、鍵センタのアドレスにアクセスし、料金決済のための認証および決済処理を行い、情報識別子IDiに対応する鍵Ksecを得て（ステップ6）、情報本体＝秘密鍵暗号方式Fsec（データ部Dsec、鍵Ksec）により情報本体を得ることができる（ステップ7）。

【００２６】

【発明の効果】以上説明したように、本発明によれば、任意の情報を任意のユーザが自由に登録し、暗号により情報を保護した状態でネットワーク上を自由に流通させることができ、情報の参照時に料金決済を行い、復号鍵を配布することにより情報を参照することを可能とする。また、良く参照される情報をネットワークの近くの場所に置いたり、分類し直して分かりやすい場所に整理することも可能であり、さらに情報を自身の計算機に置いておき、参照または使用する毎に情報料金を支払う利用形態にも適用可能となる。

【図面の簡単な説明】

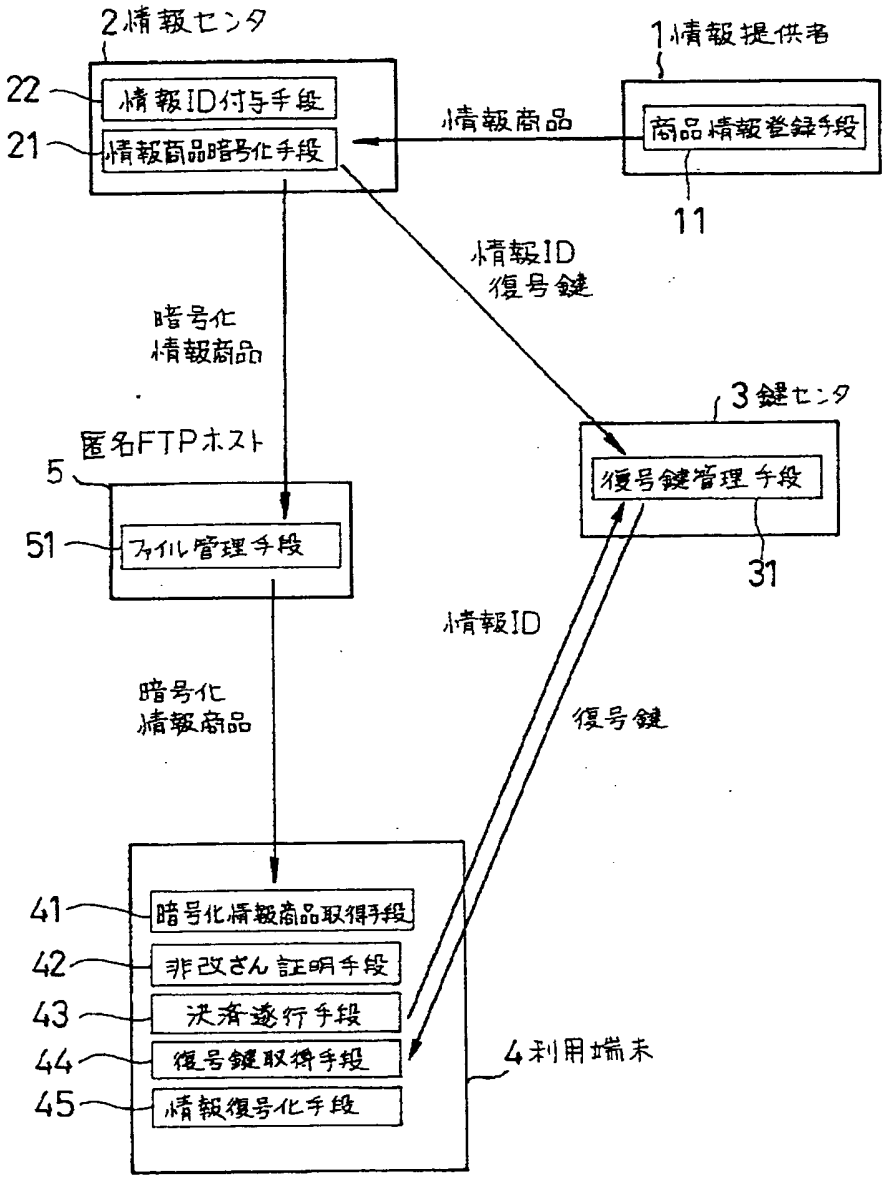
【図1】実施例の構成を示すブロック図

【図2】実施例の構成における動作手順を示すフローチャート

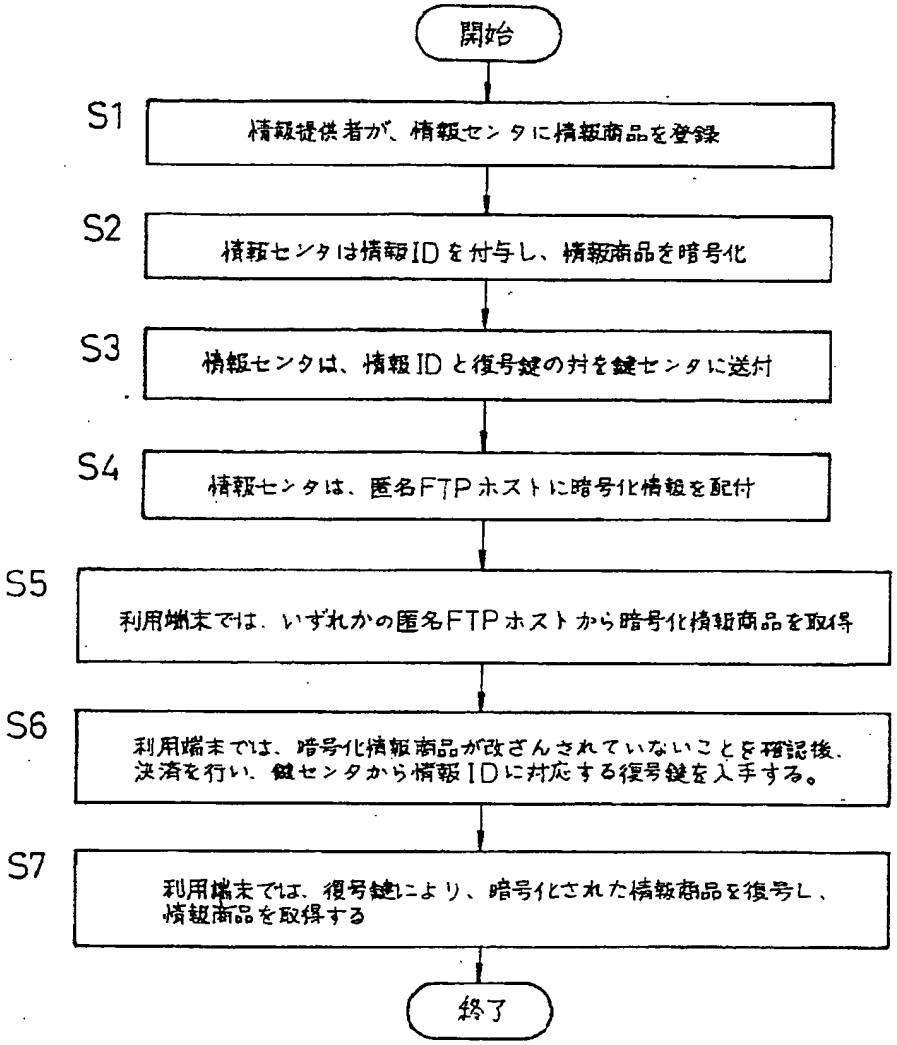
【符号の説明】

1　情報提供者
11　商品情報登録手段
2　情報センタ
21　情報商品暗号化手段
22　情報ID付与手段
3　鍵センタ
31　復号鍵管理手段
4　利用端末
41　暗号化情報商品取得手段
42　非改ざん証明手段
43　決済遂行手段
44　復号鍵取得手段
4.5　情報復号化手段
5　匿名FTPホスト
51　ファイル管理手段

【図1】


2情報センタ
1情報提供者
22
情報ID付与手段
21
情報商品暗号化手段
情報商品
商品情報登録手段
11
情報ID
復号鍵
暗号化
情報商品
3鍵センタ
匿名FTPホスト
5
復号鍵管理手段
51
ファイル管理手段
31
情報ID
暗号化
情報商品
復号鍵
41
暗号化情報商品取得手段
42
非改ざん証明手段
43
決済遂行手段
44
復号鍵取得手段
45
情報復号化手段
4利用端末

【図2】


開始
S1
情報提供者が、情報センタに情報商品を登録
S2
情報センタは情報IDを付与し、情報商品を暗号化
S3
情報センタは、情報IDと復号鍵の対を鍵センタに送付
S4
情報センタは、匿名FTPホストに暗号化情報を配付
S5
利用端末では、いずれかの匿名FTPホストから暗号化情報商品を取得
S6
利用端末では、暗号化情報商品が改ざんされていないことを確認後、決済を行い、鍵センタから情報IDに対応する復号鍵を入手する。
S7
利用端末では、復号鍵により、暗号化された情報商品を復号し、情報商品を取得する
終了